WHAT IS CLAIMED:

1. A method for establishing a trust relationship with a remote node, comprising:

generating a local public value and a local private value on at least one node;

receiving a public value from another node via an out-of-band mechanism; and

generating a secret value using the local private value in combination with the public value received from the other node.

2. A method according to Claim 1, wherein the method is performed on both of a pair of nodes, and wherein further the secret values generated at both of the nodes are symmetric.

3. A method according to Claim 2, wherein the generating a secret value includes performing a Diffie-Hellman computation.

4. A method according to Claim 1, further comprising:

retaining the secret value locally;

protecting the secret value using the public value received from the other node; and

transmitting the protected secret value to the other node via the out-of-band mechanism.

5. A method according to Claim 4, wherein the generating a secret value includes performing a Rivest-Shamir-Adleman (RSA) computation.

6. A method according to Claim 1, wherein the receiving of the public value from the other node via an out-of-band mechanism includes receiving the public value over an asynchronous connection.

7. A method according to Claim 1, wherein the receiving of the public value from the other node via an out-of-band mechanism includes downloading the public value from an external device.

8. A method according to Claim 7, wherein the external device is any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

9. A computer-readable medium having one or more instructions causing one or more processors to:

generate a local two-part code having a public code component and private code component;

receive a public code component from another processor via a peripheral device; and

generate a secret value using the local private code component and the public code component received from the other processor.

10. A computer-readable medium according to Claim 9, wherein the one or more instructions are executed on the other processor, and wherein further the secret value is symmetrical to the secret value generated on the other processor.

11. A computer-readable medium according to Claim 9, wherein the one or more instructions to generate a secret value includes one or more instructions to perform a Diffie-Hellman computation.

12. A computer-readable medium according to Claim 9, further comprising one or more instructions causing one or more processors to:

encode the secret value using the public code component received from the other processor; and

transmit the encoded secret value to the other processor via the peripheral device.

13. A computer-readable medium according to Claim 12, wherein the one or more instructions to generate a secret value includes one or more instructions to perform an RSA computation.

14. A computer-readable medium according to Claim 9, wherein the peripheral device is asynchronously connected to the one or more processors.

15. A computer-readable medium according to Claim 9, wherein the one or more instructions to receive the public code component from the other processor via

the peripheral device includes downloading the public code component from one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

16. An apparatus, comprising:

a key generator to generate a local public/private key pair; and

a shared secret generator to receive a public key from another node via an out-of-band connection and to generate a shared secret using the local private key and the public key received from the other node.

17. An apparatus according to Claim 16, wherein the shared secret is symmetrical to a shared secret generated on the other node using the local public key and a private key corresponding to the other node.

18. An apparatus according to Claim 16, wherein the other node is a server.

19. An apparatus according to Claim 16, wherein the shared secret generator is to generate a shared secret by performing a Diffie-Hellman computation.

20. An apparatus according to Claim 16, further comprising an encoder to encode the secret value using the public key received from the other node and to transmit the encoded secret value to the other node via the out-of-band connection.

21. An apparatus according to Claim 20, wherein the shared secret generator is to generate a shared secret by performing an RSA computation.

22. An apparatus according to Claim 16, wherein the out-of-band connection includes any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

23. A protocol for establishing trust between two or more processing nodes, comprising:

generating a public key and a private key on each of at least two nodes;

exchanging the public keys between the at least two nodes using an asynchronous mechanism; and

calculating a secret to be shared on at least one of the two nodes.

24. A protocol according to Claim 23, wherein the calculating of the secret to be shared includes performing a function using the public key from the other of the two nodes and the private key.

25. A protocol according to Claim 24, wherein the calculating the secret to be shared includes performing a Diffie-Hellman calculation.

26. A protocol according to Claim 24, wherein the secret to be shared is symmetrical on the at least two nodes.

27. A protocol according to Claim 23, further comprising:

encoding the secret to be shared using the public key from the other of the two nodes; and

transmitting the encoded secret to be shared to the other of the two nodes via the asynchronous mechanism.

28. A protocol according to Claim 27, wherein the calculating the secret to be shared includes performing an RSA calculation.

29. A protocol according to Claim 23, wherein the out-of-band mechanism includes any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

30. An apparatus, comprising:

means for generating a local public/private key pair; and

means for receiving a public key from another node via an out-of-band connection; and

means for generating a shared secret using the local private key and the public key received from the other node.

31. An apparatus according to Claim 30, wherein the means for generating a shared secret performs a Diffie-Hellman computation.

32. An apparatus according to Claim 30, further comprising means for encoding the shared secret using the public key received from the other node.

33. An apparatus according to Claim 32, wherein the means for generating a shared secret performs an RSA computation.

34. An apparatus according to Claim 30, wherein the out-of-band connection includes any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.